For Public Distribution

Memo

Re: An Assessment of the Open Wireless Defense

Introduction

We have been asked to prepare a memorandum on the viability of the Open Wireless Defense in the context of civil copyright infringement claims.

Background

The Open Wireless Defense is often considered by defense counsel on behalf of clients accused of illegally downloading copyrighted works via a wireless computer network. In short, the Open Wireless Defense is a claim that a third party surreptitiously accessed a defendant's unsecured wireless network and illegally downloaded a plaintiff's copyrighted works.

Summary

Based on an extensive review of applicable case law and secondary materials, we conclude that the Open Wireless Defense has never been successfully used by a defendant to escape liability for claims of direct or indirect copyright infringement. First, proving that a given wireless network was unsecured on a past date has proven to be prohibitively difficult, not to mention expose a defendant to liability for spoliation of evidence. Second, the defense has been rejected by the courts in every context in which it has been raised. Finally, the defense does not trump the "willful blindness" doctrine in the indirect copyright infringement context.

Discussion

We begin our discussion by describing the logistical difficulty of proving the Open Wireless Defense. Then, we discuss the treatment the Open Wireless Defense has received in the courts. Finally, we analyze the "willful blindness" doctrine as it relates to indirect copyright infringement and the Open Wireless Defense.

Proving the Open Wireless Defense

As its name implies, a key element of the Open Wireless Defense is that a defendant's wireless network lacked an authentication scheme (and was thus accessible by third parties within signal range) on the date that infringing activity was observed on the defendant's network. According to our technical consultants, it is extremely challenging to prove that a given network was unsecured on a past date – even if a defendant refrained from destroying all applicable network traffic logs. First, most network traffic logs cannot distinguish between authorized and unauthorized traffic. Second, even if a log is able to so distinguish, it is often the case that BitTorrent packets are encrypted and thus not subject to

Exhibit B

ready analysis. Finally, the cost of decrypting such packets and analyzing network traffic logs in preparation of litigation is often cost prohibitive.

In addition, although the vast majority of wireless routers are capable of logging network traffic, few individuals bother to enable that feature – even after they are notified of impending litigation. **Because of this, the instant such individuals raise the Open Wireless Defense, they invite a spoliation of evidence claim**. Courts have not hesitated to penalize copyright infringement defendants for their failure to retain evidence. *See Arista Records v. Tschirhart,* No. SA-05-CA-372-OG, 241 F.R.D. 462, 466 (W.D. Tex. Aug. 23, 2006). "In this case, defendant's conduct shows such blatant contempt for this Court and a fundamental disregard for the judicial process that her behavior can only be adequately sanctioned with a default judgment. No lesser sanction will adequately punish this behavior and adequately deter its repetition in other cases."

Rather than wade into the morass of the Open Wireless Defense, courts often simply prevent a defendant from raising it. *See Interscope Records v. Leadbetter*, No. 03 CV 4465 (DGT/RML), 2007 WL 1217705, at *8 n.8 (W.D. Wash. 2007); *Capitol Records Inc. v. Thomas-Rasset*, No. 06-1497 (MJD/RLE), 2009 WL 1664468, at *7 (D. Minn. June 11, 2009);

The Open Wireless Defense in the Courts

The Open Wireless Defense arises most frequently on motions to suppress evidence based on lack of probable cause. For example, in *United States v. Perez*, 484 F.3d 775 (5th Cir. 2007), a woman reported receiving an internet message containing child pornography from an individual with the Yahoo ID, "famcple." The police contacted the FBI, and a subpoena to Yahoo!, Inc. revealed that on the date the child pornography was sent, the transmitting computer used IP address 24.27.21.6. Through a second subpoena to an internet service provider, the FBI determined that the account holder associated with the IP address was Perez. A search warrant was obtained to search Perez's residence, and child pornography was found. Perez objected to the search warrant, arguing that mere association between an IP address and a physical address is insufficient to establish probable cause. He argued that because his wireless network was unsecured, other individuals could have connected to the Internet through his router and, consequently, used his IP address. **The Fifth Circuit flatly rejected Perez's argument, stating that "through it was possible that the transmissions originated outside of the residence to which the IP address was assigned, *it remained likely* that the source of the transmissions was inside that residence." *Id.* at 740 (emphasis added).**

In general, federal courts routinely deny motions to suppress based on an open wireless argument, holding that there was probable cause to search and seize defendant's computers. *See, e.g.*, *United States v. Carter*, 549 F. Supp. 2d 1257, 1268-69 (D. Nev. 2008) ("[T]he Court agrees that … there would still have remained a likelihood or fair probability that the transmission emanated from the subscriber's place of residence and that evidence of child pornography would be found at that location."; *United States v. Merz*, 2009 WL 1183771, at *5 (E.D. Pa. May 4, 2009) ("The court also concludes there was a sufficient connection between the IP address … and the physical location to which the IP address was linked to establish probable cause to search the physical location."). *See also*, *United States v. Massey*, No. 4:09CR506-DJS, 2009 WL 3762322 (E.D. Mo. Nov. 10 2009); *United States v. Hibble*, No. CR 05-1410 TUC DCB (HCE), 2006 WL 2620349 (D. Ariz. Sept. 11, 2006).

The Open Wireless Defense has also been raised by defendants in civil copyright infringement actions. In *Arista Records, Inc. v. Musemeci*, the defense arose on a motion to vacate summary judgment. No. 03 CV 4465, 2007 WL 3124545, at *5 (E.D.N.Y. Sept. 18, 2007). **The court concluded that the defendant's claim that an unsecured wireless router at his residence could have been used by an outside party to commit the alleged infringing activity was not a meritorious defense and denied the motion.** *Id*. In *Capitol Records, Inc. v. Thomas-Rasset*, the court excluded expert testimony on the Open Wireless Defense because the defendants were unable to offer sufficient evidence in its support. No. No. 06-1497 (MJD/RLE), 2009 WL 1664468, at *7 (D. Minn. June 11,

2009). In *Interscope Records v. Leadbetter*, the Open Wireless Defense was similarly excluded. No. 03 CV 4465 (DGT) (RML), 2007 WL 1217705, at *8 n.8 (W.D.Wash. 2007).

Secondary Liability and the "Willful Blindness" Doctrine

The unlikely defendant who escapes liability for direct copyright infringement vis-à-vis the Open Wireless Defense will nevertheless have to contend with liability for contributory copyright infringement. Contributory infringement occurs when a party who, with knowledge of the infringing activity, induces causes, or materially contributes to the infringing conduct of another. *Metro-Goldwyn Mayer Studios, Inc. v. Grokster, Ltd.*, 545 U.S. 913 (2005); *Gershwin Pub. Corp. v. Columbia Artists Management, Inc.*, 443 F.2d 1159, 1162 (2d Cir. 1971).

A defense counsel's first instinct is to allege that a client is innocent where a client had no actual knowledge that the conduct it engaged in (i.e. providing internet access to copyright infringers) constituted contributory infringement. Before advancing those claims, however, an attorney would be well advised to take a close look at the conduct for which persons engaging in infringing activity have been held responsible. Because the typical wireless router is readily capable of logging traffic, a defendant cannot escape liability by claiming they never made the effort to analyze such traffic. Willful blindness is knowledge. *In re Aimster Copyright Litigation*, 334 F.3d 643, 654 (7th Cir. 2003); *Deep v. Recording Industry Ass'n of America, Inc.*, 540 U.S. 1107 (2004).

Thus, an internet account holder who maintains a wireless network and fails to monitor the traffic on the network is liable for contributory copyright infringement. *Id*. Copyright law may lead to harsh results, but it nevertheless is the law.

Conclusion

The Open Wireless Defense is not viable. First, from a technical standpoint it is extremely challenging to establish that a wireless network was unsecured on a past date and if the related evidence has not been preserved then a defendant may be subject to liability for spoliation of evidence upon raising the defense. Second, it has never been successfully used to avoid liability for direct copyright infringement in any court in the United States. Finally, even if it were established that a third party used an account holder's internet account to illegally download copyright content, the account holder would not be able to escape liability for contributory copyright infringement.